

REMARKS

This Amendment is submitted in answer to the Office Action dated December 27, 2007, having a shortened statutory period set to expire March 27, 2008, extended to April 27, 2008.

I. Rejection under 35 USC § 112, first paragraph

In paragraph 5 of the present Office Action, Claims 1, 9 and 17 are rejected under 35 U.S.C. § 112, 1st paragraph, as failing to comply with the written description requirement. In particular, the Examiner believes “[t]here is no specific disclosure ‘, wherein said associated key comprises a key that is not publicly published.’” In response, Applicant respectfully traverses the Examiner’s rejection because the specification contains written description supporting the recitation in amended exemplary Claims 1, 9 and 17 of “said associated key comprises a private key.”

Turning now to the specification, Applicant respectfully points out that block 310 of Figure 3 and the corresponding description at page 15, lines 25-27 explicitly disclose, “Block 310 illustrates server system 104 encrypting user key 1 with PRKA of associated key A stored in server system 104.” The term PRKA is defined at page 10, line 33 through page 11, line 2 as a “private key A.” Thus, the rejection under 35 U.S.C. § 112, 1st paragraph, is overcome because the amended claim language has clear support in the written description in the specification.

II. Rejection under 35 USC § 103

In paragraph 7 of the present Office Action, Claims 1-4, 6-12, 14-20 and 22-24 are rejected under 35 U.S.C. § 103 as unpatentable over U.S. Patent No. 6,807,277 to *Doonan et al. (Doonan)* in view of U.S. Patent No. 6,732,101 to *Cook*. In addition in paragraph 8, Claims 5, 13 and 21 are rejected under 35 U.S.C. § 103 as unpatentable over *Doonan* and *Cook* in view of U.S. Patent No. 4,888,800 to *Marshall*. Those rejections are respectfully traversed, and favorable reconsideration of the claims is requested.

The combination of *Doonan* and *Cook* does not render exemplary Claim 1 (and similar Claims 9 and 17) of the present invention unpatentable under 35 U.S.C. § 103 because the

combination of cited references does not disclose each feature recited therein. For example, the combination of *Doonan* and *Cook* does not disclose the following step of exemplary Claim 1 as amended:

storing an associated key in the encrypting data processing system and encrypting the user key with the associated key to obtain an encrypted user key, wherein said associated key comprises a private key.

With respect to the claimed “associated key”, page 3 of the present Office Action cites col. 5, lines 63-67 of *Doonan*, which disclose:

The composite message P is first encrypted to form encrypted message Pe, using a randomly-generated symmetric encryption key Ks. The symmetric key Ks is then itself encrypted using the public key published in a digital certificate owned by the recipient, to form [the encrypted symmetric key] Kp. (emphasis supplied)

Thus, *Doonan’s public key of the message recipient* is relied upon in the present rejection as disclosing the claimed “associated key.” However, as made clear by the amendments made herein, the claimed “associated key comprises a private key,” rather than a public key as disclosed by *Doonan*. Consequently, the combination of *Doonan* and *Cook* does not disclose each claimed feature and therefore does not render the present claims unpatentable under 35 U.S.C. § 103.

Applicant further respectfully submits that the combination of *Doonan* and *Cook* does not render exemplary Claim 1 unpatentable under 35 U.S.C. § 103 because that combination of references does not disclose the following step of exemplary Claim 1 as amended:

thereafter, preventing validation of the association of the user with messages by revoking the associated key at the encrypting data processing system so that the encrypting data processing system is no longer able to decrypt the encrypted user key. [emphasis supplied]

With reference to the step of “preventing validation of the association of the user with messages”, page 6 of the present Office Action correctly notes that *Doonan* does not disclose revocation of an associated key as claimed. However, the Office Action then relies upon *Cook’s* disclosure of the conventional deletion of a key by a signature manager 132 at col. 6, lines 40-50:

Signature manager 132 is a utility for managing encryption keys for a user. Prior to the use of wrapping application 128 or viewer 130, each user (e.g., sender 102 or fully configured recipient 104a) must generate public and private keys. Signature manager 132 includes methods for generating public and private keys. Signature manager 132 submits the public key to key server 108 for publication. Key server 108 publishes the public keys in a key list which in turn can be distributed to key retrieval servers 180. Signature manager 132 can be used to create new keys, change keys, delete keys or change signature phrases. [Emphasis supplied]

The combination of *Doonan* and *Cook* urged by the Examiner thus requires a signature manager 132 at the encrypting (i.e., sender) data processing system to delete the public key of a message recipient. As should be apparent, the simple deletion at the sender (i.e., encrypting) system of a message recipient's public key does not "prevent[] validation of the association of the user with messages" and does not render the encrypting data processing system unable "to decrypt the encrypted user key" as claimed. Instead, a user of the sender system can easily again access the recipient's public key at any time utilizing *Cook*'s key retrieval server 180, as taught by *Cook* at col. 6, lines 40-50, and thereby again access the encrypted user key. Thus, the combination of *Doonan* and *Cook* does not render obvious the claimed step of "preventing validation of the association of the user with messages" recited in exemplary Claim 1.

In view of the failure of the combination of *Doonan* and *Cook* to disclose each feature recited in exemplary Claim 1, Applicant respectfully submits that Claim 1, similar Claims 9 and 17 and their respective dependent claims are not rendered unpatentable under 35 U.S.C. § 103.

Having now responded to each rejection set forth in the present Office Action, Applicant believes all pending claims are now in condition for allowance and respectfully requests such allowance. No additional fee is believed to be required; in the event any additional fee is required, please charge such fee to Dillon & Yudell LLP Deposit Account No. **50-3083**.

Respectfully submitted,



Brian F. Russell
Registration No. 40,796
DILLON & YUDELL LLP
8911 N. Capital of Texas Hwy., Suite 2110
Austin, Texas 78759
(512) 343-6116
ATTORNEY FOR APPLICANT